ST. CATHERINE'S EARLY EDUCATION CENTRE

CYBER SAFETY POLICY

Cyber safety is the safe and responsible use of Information and Communication Technologies (ICT). It involves being respectful of other people online, using good 'netiquette' (internet etiquette), and is about keeping information safe and secure to protect the privacy of individuals. Our Service is committed to create and maintain a safe online environment with support and collaboration from staff, families and community. As a child safe organisation, our Service embeds the Child Safe Standards and continuously address risks to ensure children are safe in physical and online environments.

National Quality Standard (NQS)

Quality Area 2: Children's Health and Safety		
2.2	**safety**	Each child is protected
2.2.1	**Supervision**	At all times, reasonable precautions and adequate supervision ensure children are protected from harm and hazard.
2.2.3	**Child Protection**	Management, educators and staff are aware of their roles and responsibilities to identify and respond to every child at risk of abuse or neglect.

Quality Area 7: Governance and Leadership		
7.1.2	**Management system**	Systems are in place to manage risk and enable the effective management and operation of a quality service.

Education and Care Services National Regulations

84	**Awareness of child protection law**
168	Education and care services must have policies and procedures
181	Confidentiality of records kept by approved provider
195	Application of Commonwealth Privacy Act 1988
196	Modifications relating to National Education and Care Services Privacy Commissioner and Staff

Related Policies

Child safe environment policy
Dealing with complaints policy
Enrolment policy
Code of Conduct policy
Fraud prevention policy
Technology usage policy
Privacy and confidentiality policy
Record keeping and retention policy

PURPOSE

Our centre creates and maintains a cyber safe culture that works in conjunction with our service philosophy, privacy and legislative requirements to ensure the safety of enrolled children, educators and families.

SCOPE

This policy applies to children, families, educators, staff, management, students, volunteers and visitors, approved provider of the Service.

IMPLEMENTATION

Cyber Safety encompasses the protection of users of technologies that access the Internet, and is relevant to devices including computers, iPads and tablet computers, mobile and smart phones and any other wireless technology (including personal wearable devices- smart watches). With increasingly sophisticated and affordable communication technologies, there is a candid need for children and young people to be informed of both the benefits and risks of using such technologies. More importantly, safeguards should be in place to protect young children from accidentally stumbling upon or being exposed to unsuitable material or content.

CCS Software

- Our Service uses Xplor which is a third-party software system to access the Child Care Subsidy System (CCSS). The software is used to manage the payment and administration of the Child Care Subsidy (CCS).

The approved provider will review any potential threats to software security on a monthly basis. The director/ nominated supervisor will advise the approved provider as soon as possible regarding any potential threat to security information and access to data sensitive information. Any breaches of data security will be notified to the Office of the Australian Information Commissioner (OAIC) by using the online Notifiable Data Breach Form.

- All Personnel using the software will have their own log in username and password. The approved provider will ensure all personnel using the software will have their own log-in username and password.
- Each personnel who is responsible for submitting attendances and enrolment notices to CCS will be registered with PRODA as a Person with Management or Control of the Provider or as a Person with Responsibility for the Day-to-Day Operation of the Service.

REVIEW OF CCS SOFTWARE PROCEDURE:

Review	How Often	By Whom
All Management use an individual log-in to access CCS software	As required	Approved provider and director/ Business Manager/Assistant Director
Privacy policy of CCS software	As required	Approved provider and Management
Any breaches of sensitive data relating to Enrolments	Upon notification	Approved provider and Management team

Privacy and Confidentiality

- The principles of confidentiality and privacy extend to accessing or viewing and disclosing information about personnel, children and/or their families, which is stored on the Service's network or any device
- Privacy laws are such that educators or other employees should seek advice from Service management regarding matters such as the collection and/or display/publication of images (such as personal images of children or adults), as well as text (such as children's personal writing)
- A permission to publish form must be signed by parent/guardians to ensure children's privacy, safety and copyright associated with the online publication of children's personal details or work

- Department of Education NSW guidelines are followed regarding issues of privacy, safety, and copyright associated with the online publication of children's personal details or work
- All material submitted for publication on the Service Internet/Intranet site should be appropriate to the Service's learning environment
- Material can be posted only by those given the authority to do so by the Service management
- The Service management should be consulted regarding links to appropriate websites being placed on the Service's Internet/Intranet (or browser homepages) to provide quick access to sites.

The Approve Provider/Nominated Supervisor/ Management will Ensure:

- Ensure obligations under the *Education and Care Services National Law and National Regulations* are met
- All educators, staff, students, visitors and volunteers have knowledge of and adhere to this policy and associated procedure
- All staff, families and visitors are aware of the Service's *Code of Conduct* and *Confidentiality and Privacy Policies*
- The Service works with an ICT (Information and communication technologies) security specialist to ensure the latest security systems (Microsoft Defender) are in place to ensure best practice. Anti-virus and internet security systems including Hardwall firewalls can block access to unsuitable web sites, newsgroups and chat rooms. However, none of these tools are fool proof; they cannot be a substitute for active adult supervision and involvement in a child's use of the internet
- Backups of important and confidential data are stored weekly
- Backups are stored securely in IDRIVE.COM with zero knowledge of encrypted data (using a cloud-based service)
- Software and devices are updated regularly to avoid any breach of confidential information
- Families are referred to the *Dealing with Complaints Policy* and procedure when raising concerns regarding digital technologies and personal data

- All staff are aware that a breach of this policy may initiate appropriate action including the termination of employment
- Notification is made to the Office of the Australian Information Commissioner (OAIC) by using the online Notifiable Data Breach Form in the event of a possible data breach. This could include:
    - a device containing personal information about children and/or families is lost or stolen (parent names and phone numbers, dates of birth, allergies, parent phone numbers)
    - a data base with personal information about children and/or families is hacked
    - personal information about a child is mistakenly given to the wrong person (portfolios, child developmental report)
    - this applies to any possible breach within the Service or if the device is left behind whilst on an excursion

Educators will:

- Ensure to use appropriate and acceptable way and stay safe online by adhering to Service policies and procedures
- Keep passwords confidential and not share with anyone
- Log out of sites to ensure security of information
- Never request a family member's password or personal details via email, text, or Messenger
- Report anyone who is acting suspiciously or requesting information that does not seem legitimate or makes you feel uncomfortable
- Obtain parent permission for children to use computers as part of the enrolment procedure
- Ensure that children are never left unattended whilst a computer or mobile device is connected to the internet.
- ensure personal mobile phones are not used to take photographs, video or audio recordings of children at the Service
- Only use educational software programs and apps that have been thoroughly examined for appropriate content prior to allowing their use by children.
- Provide parents and families with information about the apps or software programs accessed by children at the Service

- Participate in professional development regarding online safety
- provide online safety for children by adhering to policies and procedures that align to the National Child Safety Principles- Child Safe Standards
- Ensure that appropriate websites are sourced for use with children **prior** to searching in the presence of children
- ensure privacy filters and parental control settings are turned on and used when children are accessing digital technologies online.
- Provide education to the children on the cyber safety in a simple way

Families will:

- Be aware that when sharing anything using technologies such as computers, mobile devices, email, or any device that connects to the internet, you and everyone else invited to your account understands about *security* and staying safe online and ensures privacy laws are adhered to.
- Be aware that when it comes to your own children, it is your choice what you share outside of the Service. Remember though that young children cannot make their own decisions about what gets published online so you have a responsibility to ensure that whatever is shared, is in your children's best interests
- Be mindful of what you publish on social media about your child as this may form part of their lasting digital footprint
- Consider installing Family friendly filters to limit access to certain types of content on devices such as mobile phones and computers
- Consider installing parental controls on streaming services to ensure children are not able to access inappropriate material
- consider developing a *Family Tech Agreement* to establish rules about use of devices at home
- Be aware that sometimes other children in the Service may feature in the same photos, videos, and/or observations as their children. In these cases, Families are never to duplicate or upload them to the internet/social networking sites or share them with anyone other than family members
- access further information about eSafety to help protect their children and be cyber safe.

BREACH OF POLICY

- Staff members or educators who fail to adhere to this policy may be in breach of their terms of employment and may face disciplinary action. Visitors or volunteers who fail to comply to this policy may face termination of their engagement.

RESOURCES

Australian Government Office of the e Safety commission https://www.esafety.gov.au/educators
E Safety Early Years Online safety for under 5s.
https://www.esafety.gov.au/sites/default/files/2020-02/Early-years-booklet.pdf
Family Tech Agreement. E Safety Early Years Online safety for under 5s
https://www.esafety.gov.au/sites/default/files/2020-01/Our%20Family%20Tech%20Agreement_0.pdf
Kiddle is a child-friendly search engine for children that filters information and websites with deceptive or explicit content: https://www.kiddle.co/
Receive information on scams that can then be provided to the public. To report an online scam or suspected scam, use the form found here: https://www.scamwatch.gov.au/report-a-scam
More information on online fraud and scams can be found on the Australian Federal Police website https://www.afp.gov.au/what-we-do/crime-types/cyber-crime
Notifiable Data Breaches scheme (NDB) can be made through the Australian Government Office of the Australian Information Commissioner

CONTINUOUS IMPROVEMENT/REFLECTION

Our *Cyber Safety Policy* will be reviewed on regular basis in consultation with children, families, staff, educators and management.

Source

Australian Children's Education & Care Quality Authority. (2014).
Australian Children's Education & Care Quality Authority. (2023). Guide to the National Quality Framework.
Australian Government e Safety Commission (2020) www.esafety.gov.au
Australian Government Department of Education. *Child Care Provider Handbook (2023)*
https://www.education.gov.au/early-childhood/resources/child-care-provider-handbook

Australian Government Office of the Australian Information Commissioner (2019)
https://www.oaic.gov.au/privacy/notifiable-data-breaches/about-the-notifiable-data-breaches-scheme/
Early Childhood Australia Code of Ethics. (2016).
Education and Care Services National Law Act 2010. (Amended 2023).
Education and Care Services National Regulations. (Amended 2023).
Privacy Act 1988.
Revised National Quality Standard (2018)

Review
This policy will be reviewed regularly.
The review will be conducted by:

- Management
- Employees
- Families
- Interested Parties

Date Reviewed	**Modifications**	**Next Policy Review Date**
July 2022	This policy was created	July 2023
July 2023	Sources checked and links updated Legislation updated Continuous improvement /reflection section added Policy maintenance Breach of policy section added	July 2025